

УДК 330.658.005.5

Сотниченко В.М.

кандидат педагогічних наук, доцент,  
завідувач кафедри підприємництва, торгівлі та біржової діяльності  
Державного університету телекомунікацій, м. Київ

## ПОЛІТИКО-ПРАВОВІ ОСНОВИ УПРАВЛІННЯ ЕКОНОМІЧНОЮ БЕЗПЕКОЮ ТЕЛЕКОМУНІКАЦІЙНИХ ПІДПРИЄМСТВ

### POLITICAL LEGAL FOUNDATION OF THE MANAGEMENT OF ECONOMIC SECURITY OF TELECOMMUNICATION ENTERPRISES

#### АНОТАЦІЯ

У статті розглянуто окремі аспекти політико-правового регулювання процесу розбудови в Україні цифрової економіки. Акцентовано увагу на основах управління економічною безпекою телекомунікаційних підприємств. Надано оцінку стану економічної безпеки підприємств галузі. Наведено дані про характер загроз та тенденції розвитку телекомунікацій. Наголошено на необхідності більш динамічної процедури імплементації європейських рішень, важливих для розвитку єдиного ринку України та ЄС.

**Ключові слова:** економічна безпека, цифрова економіка, телекомунікаційне підприємство, стратегія цифрового ринку, інформаційно-комунікаційні технології, кібербезпека.

#### АННОТАЦИЯ

В статье рассмотрены отдельные аспекты политико-правового регулирования процесса развития в Украине цифровой экономики. Акцентируется внимание на основах управления экономической безопасностью телекоммуникационных компаний. Дана оценка состояния экономической безопасности предприятий отрасли. Приведены данные о характере угроз и тенденции развития телекоммуникаций. Отмечена необходимость более динамичной процедуры имплементации европейских решений, важных для развития единого рынка Украины и ЕС.

**Ключевые слова:** экономическая безопасность, цифровая экономика, телекоммуникационное предприятие, стратегия цифрового рынка, информационно-коммуникационные технологии, кибербезопасность.

#### ANNOTATION

The article deals with some aspects of political and legal regulation development process in Ukraine digital economy. The attention based on management of economic security of telecommunication companies. The estimation of the state of the economic security of the industry. The data on the nature of the threats and trends in the development of telecommunications. There was a need for a more dynamic implementation of the procedures of the European decisions that are important for the development of a single market in Ukraine and the EU.

**Keywords:** economic security, digital economy, telecommunications company, strategy of the digital market, ICT, cyber.

**Постановка проблеми.** В основі прогресивного розвитку сфери електронних комунікацій, розбудови вітчизняної телекомунікаційної інфраструктури, сучасних технологій знаходяться світові тенденції розвитку інформаційно-комунікаційних технологій. На сьогодні більше 3% ВВП України складає частка ІКТ, а інформаційні та телекомунікаційні послуги в країні – це п'ята частина вітчизняного ринку. За підсумками зовнішньої торгівлі 2016 року на експорті ІТ – послуг Україна заробила \$1,6 млрд.

Однак наміченої мети перетворення національної економіки на цифрову Україна не досягла і відстає в цьому від багатьох країн, втрачає

позиції за показниками рейтингового оцінювання міжнародних організацій – Всесвітнього економічного форуму ООН та Міжнародного союзу електрозв'язку. Особливо, що стосується прямих іноземних інвестицій, розвитку електронного врядування, розвитку ІКТ. На сьогодні немає чітко виробленої концептуальної основи дієвої взаємодії між ІТ-бізнесом і державою.

**Постановка завдання.** Основним завданням автора під час написання статті є накреслення напрямів і тенденцій розбудови цифрового суспільства в Україні, переведення національної економіки в цифрову. Звернути увагу на першочергові питання політико-правового регулювання економічної безпеки телекомунікаційних підприємств. Зробити наголос на інвестиційну непривабливість України через слабку систему захисту економіки від кіберзагроз.

**Аналіз останніх досліджень і публікацій.** Питання захисту економічних інтересів підприємств, дотримання необхідного рівня економічної безпеки сьогодні актуальні для всього цивілізованого світу. Поняття «кібербезпека», «економічна безпека», «цифрова економіка», «телекомунікаційне підприємство», «інфраструктура телекомунікацій» стали брендовими в наукових дослідженнях багатьох зацікавлених цією проблемою науковців. Але в контексті завдань цієї статті найбільш актуальними є думки таких авторів як О. Гудзь, Т. Зубко, Т. Макаренко, І. Новикова, А. Янковський, Н. Ястремська, Л. Фролова.

О. Гудзь приділяє увагу гармонізації механізмів управління інноваційним розвитком підприємств. Проблеми розбудови привабливого інвестиційного простору, пошуки шляхів і механізмів для вирішення цього завдання, конкурентоспроможність підприємств зв'язку є предметом наукових інтересів Т. Макаренко, І. Новикової. Цікавими і надзвичайно актуальними є проблеми розбудови ринку інфокомунікаційних технологій, товарів і послуг. Дослідження цього напрямку належить авторам Н. Ястремській і Л. Фроловій, А. Янковський – у своїх публікаціях на сторінках інтернет-видань гостро ставить питання створення в Україні надійної системи захисту від кіберзагроз.

**Виклад основного матеріалу дослідження.** Кількість активних користувачів Інтернету в

Україні на початок 2017 року складала близько 60% населення України. Решта населення знаходиться під впливом, а скоріше в прямій залежності від інформаційно-комунікаційних технологій, які проникають практично у всі сфери життя. Але, очевидним є той факт, що телекомунікації набирають обертів у своєму розвитку.

У країні спостерігається позитивна динаміка зростання доходів у галузі телекомунікацій, але це навіть не покриває рівня інфляції. Плюс до того, більше 70% ринку послуг займають чотири великі оператори, що свідчить про відсутність наявного зростання, яке може бути забезпечено лише розробкою і впровадженням нових технологій [1, с. 12].

Україна втягнута в гібридну війну, але закону про кібербезпеку немає. Зміцнення кібербезпеки визнано одним із пріоритетів в українській національній Стратегії сталого розвитку «Україна–2020». За даними щорічного вивчення корпоративних ризиків, що було проведено на основі опитування 800 ризик-менеджерів і страхових агентів із 44 країн кіберзлочинність уперше увійшла в ТОП-3 корпоративних ризиків. Кіберзлочинність визначають як найбільший ризик для підприємств на довгострокову перспективу. Дослідницька компанія Cybersecurity Ventures прогнозує, що на 202 рік втрати від кіберзлочинності у світі збільшаться в рази і сягнуть \$6 трлн. Насамперед традиційно страждають фінансові організації, а також майданчики електронної комерції.

При цьому згідно з даними звіту Trend Micro Incorporated, однією з найбільш значущих загроз є банківські трояни. Вкрадена троянами інформація використовується правопорушниками для проведення шахрайських транзакцій або продається на підпільних сайтах. До того ж, у результаті цих шахрайських дій фінансові організації несуть збитки, бо повинні компенсувати своїм клієнтам вкрадені суми грошей.

Але це загроза не лише економічній безпеці телекомунікаційним підприємствам, а й національній безпеці загалом. До тих пір, поки вітчизняна економіка не захищена від кібератак, ніяких інвестицій не буде. Ніхто не захоче ризикувати своїми ресурсами.

Однак сьогодні, як ніколи раніше, зросли загрози для економічної безпеки галузі в умовах так званої гібридної війни. З одного боку, це фізичне пошкодження телекомунікаційних мереж, інфраструктури, а з іншого – посилення впливу кіберзагроз з деструктивними для галузі наслідками. Саме в цих умовах виявилася критична залежність державних структур управління та силових відомств від техніко-технологічного стану телекомунікаційної галузі. Під загрозою відверто агресивного втручання знаходиться вся система Національної безпеки України. На жаль, у напрямі зміцнення безпеки сьогодні робиться дуже мало. Україна в цьому плані практично очолює антирейтинг країн на

світовому рівні. В країні найбільш небезпечний кіберпростір.

Через недосконалість системи кіберзахисту Україна складає загрозу для цивілізованого світу. Очевидні речі, що через це ми є країною з непривабливою інвестиційною політикою [4, с. 78–85]. Більше того, самі є джерелом кібератак, різного роду шкідливих програм, ботнетів [6].

Законодавча база функціонування сфери телекомунікацій в Україні потребує суттєвого доопрацювання та оновлення. Особливо в таких напрямках як: інвестиційна політика, розподіл та користування радіочастотами і нумерацією, політика ціноутворення та якості послуг, ліцензування, спрощення дозвільних процедур тощо. Потребують вирішення у законодавчій площині і такі питання як реформування засад державного регулювання у сфері електронних комунікацій, забезпечення кібербезпеки, надання електронних довірчих послуг.

Гострим залишається і питання економічної безпеки телекомунікаційних підприємств. Ведеться робота в напрямі вирішення цього питання, кращі спеціалісти ІТ-сфери працюють над розробкою власних криптографічних алгоритмів, створення технологічної бази для запровадження на практиці електронних підписів, що є абсолютно необхідною потребою як у бізнесі, так і в захисті персональних даних, електронних інформаційних ресурсів, електронних комунікацій.

Для того, щоб створити умови для зростання, необхідно суттєво оновити законодавчу базу, особливо що стосується доступу до інфраструктури та радіочастотного ресурсу.

Те, що є економічною, національною, державною безпекою знаходиться в полі посиленої уваги і має бути захищено від кібератак. Очевидно цьому питанню не надається належного значення. Як на рівні населення, так і на рівні відповідальних за це осіб. Для того, щоб населення мало уявлення про можливі небезпеки, необхідне активне впровадження просвітницької програми. Зазвичай, особливо на рівні малого та середнього бізнесу, менеджери вирішують свої економічні питання за допомогою мобільного зв'язку. Але мало хто знає, що всі розмови телефонами Apple чи Android прослуховуються іноземними спецслужбами. Тобто інформація, що передається каналами мобільного зв'язку не захищена.

Простота і прозорість питання щодо вирішення завдань захисту економічної безпеки є очевидною. Не треба нагромодження формул, математичних викладок і занадто складних ідей як від цього захиститися. Необхідно розробити і прийняти закон про кібербезпеку й організувати на цивілізованому високо технологічному рівні захист інтересів в усіх сферах життєдіяльності людини, суспільства та держави [3, с. 81–87]. А комерційна таємниця в бізнесі, економічна безпека підприємства не в останню чергу. Успішна економіка – це запорука успішної політики, міцної держави.

Сфера телекомунікацій потребує більш ефективного законодавства. На сьогодні сферу регулюють більше 300 законів та нормативних актів. Але вони не дають очікуваного результату, оскільки в державних органах влади надзвичайно неефективно використовують технології.

Має місце практика перевищення повноважень органами влади під час перевірки ІТ-компаній, що перешкоджає успішному вирішенню завдань із захисту економічної безпеки підприємств. ІТ-компанії в Україні знаходяться під постійним наглядом і контролем, причому нерідко з незрозумілих причин. Про це на парламентських слуханнях у Верховній Раді України в лютому 2016 року наголосив голова правління Інтернет Асоціації України О.П. Федієнко. Це заважає розвитку бізнесу в галузі, робить її непривабливою для інвестицій. Із його слів, нерідко проводять обшуки, вилучають комп'ютерну техніку, сервери [1, с. 35–38; 4, с. 78–85].

Інформаційно-комунікаційні технології – це та галузь в економіці України, спираючись на яку можна зробити економічний прорив і вивести її в число країн із найбільш успішною економікою [5, с. 17–19]. Однак тривалий час на цьому шляху діють реальні перешкоди, які заважають цьому. Наприклад, лише 7 лютого 2017 року Верховна Рада України прийняла за основу і загалом законопроект «Про доступ до інфраструктури об'єктів будівництва, транспорту, електроенергетики для розвитку телекомунікаційних мереж».

Ним передбачено, що віднині всі учасники ринку телекомунікацій будуть мати рівний до нього доступ. Це більш повно сприятиме розвитку інформаційного суспільства в Україні. На сьогодні реально консолідованої позиції у власників об'єктів інфраструктури і провайдерів немає. Це є фактором загрози для економічної безпеки провайдерів, власників телекомунікаційних підприємств.

Механізм визначення вартості доступу до об'єктів інфраструктури не має економічно обґрунтованої основи, про що зазначено в пояснювальній записці до законопроекту. На сьогодні вартість доступу до інфраструктури завищено. Перед операторами і провайдерами ставлять такі цінові бар'єри, що вони ніяк не можуть бути рентабельними. Примушують витрачатися на такі невласливі для них завдання як ремонт будинків, під'їздів. Ціни для кожного конкретного випадку, для кожного окремо взятого оператора встановлюються свавільно, нерідко просто ніяк не обґрунтовано. Немає чіткої методики визначення цін. Але, на думку фахівців, що представляють Інтернет-асоціацію України (ІнАУ), цей законопроект є лише компромісним і не повною мірою вдовольняє всі сторони, враховуючи й учасників ринку телекомунікацій. Але позитивно те, що такий крок зроблено, створена законодавча основа, яка дає можливість співпрацювати більш узгоджено і надалі її вдосконалювати. А саме фор-

мування вже узаконених порядків, розробка методик та правил, а також відповідних підзаконних актів, які ще мають бути прийняті.

З погляду визначення перспективних завдань галузі та їх успішного вирішення, слід орієнтуватися, в процесі проведення реформ, на європейські засади Стратегії єдиного цифрового ринку, яка базується на такій позиції, як надійний, законодавчо захищений і досконалий онлайн-доступ до ринку товарів і послуг [7]. Для цього необхідно створювати відповідне середовище, яке б максимально сприяло розвитку цифрової мережі та послуг.

І ще однією позицією є техніко-технологічна складова, а саме розробка та впровадження передових цифрових технологій. Стратегія побудована і впроваджується у практику життя з розумінням того, що прогрес щодо розбудови цифрової України є категорією динамічною. Впровадження технологій буде впливати на формування нових стандартів. Нові стандарти вимагатимуть покращення параметрів онлайн-доступу до ринку інфокомунікаційних товарів та послуг. Зміни зазначених параметрів закономірно призведуть до необхідності змін у цифровому просторі загалом.

Прагнення України до єдиного цифрового ринку згідно Угоди про Євроасоціацію потребує вирішення важливих завдань в законодавчому плані, а саме, проведення імплементації тих європейських рішень, які насамперед є найбільш важливими для єдиного ринку України та Європейського Союзу. Водночас такий ринок має працювати мультиплікативно, оскільки створення та поширення цифрових технологій дає світу нові можливості, нові форми обробки даних для економіки [2, с. 26–32]. Змінюються методи виробництва, підвищуються показники якості й ефективності. З'являються нові моделі використання енергоресурсів і відкриваються перспективи розбудови «розумних міст». І ще один цікавий аспект – упровадження нових технологій у процесі розбудови цифрової країни дозволить більш повно врахувати потреби населення в товарах і послугах, які стануть більш персоналізованими.

Наприклад, сьогодні більше половини населення України є користувачами інтернету, користуються соціальними мережами, ведуть електронне листування. З цих каналів комунікації зацікавленим суб'єктам господарювання можна багато про що дізнатися, зокрема про потреби населення в товарах і послугах. Варто лише віртуально виявити зацікавленість товаром чи послугою через рекламу, розміщену в Інтернеті, як тут же надходить персональна пропозиція. І не обов'язково звертатися до конкретної реклами. Інтерес користувача Інтернету може бути виявлений через тематику та наповнення сайтів до яких виявляється найбільший інтерес. А це один з аспектів законодавчого врегулювання питання економічної безпеки і, безумовно, захисту персональних і корпоративних (на рівні підприємства) даних.

Інтернет радикально змінив життя в усіх аспектах, напрямках і сферах. І в приватному плані, і в соціальному, і в економічному, і в громадянському. По суті проглядається тенденція до народження нової соціоекономічної моделі розвитку. Свідченням цього прояву є гармонізація, тобто розподіл і узгодження в галузі ІКТ функцій держави та ринку інфокомунікаційних товарів і послуг.

Говорячи про захист економічної безпеки підприємств взагалі і підприємств телекомунікаційної галузі зокрема, треба виходити зі світового досвіду. У цивілізованому світі питання кібербезпеки є постійно актуальним і звичним на буденному рівні, є невід'ємною складовою повсякденного життя. Там це один із пріоритетів. Оскільки Україна прагне до євроінтеграції, питання кібербезпеки теж має стати пріоритетним, тому що це впливає на функціонування економіки, обороноздатність, на соціальну сферу, рівень життя населення.

Процес формування законодавчої бази в галузі телекомунікацій як основи її ефективного функціонування в країні йде досить повільно. Український цифровий ринок і аналогічний ринок ЄС й досі працюють за нормами і стандартами, які лишаються не узгодженими. Такий стан речей значно зменшує можливості українського ринку, заважає надходженню інвестицій [7]. Говорячи про цифровий ринок, не можна обійти значення його базової основи – телекомунікацій. Неврегульованість на законодавчому рівні окремих питань у цій галузі, перешкоджає процесу інтеграції в європейський та світовий інформаційний простір. А це робить уразливою економічну безпеку телекомунікаційних підприємств і національну економіку загалом. Прикладом може служити безпрецедентне втручання в роботу електромереж України в грудні 2015 року, коли 230 тис. жителів Прикарпаття на 6 годин лишилися без електропостачання. Диспетчер підприємства, яке розподіляє електроенергію, побачив на моніторі комп'ютера як курсор почав самостійно рухатися по екрану і самостійно відмикати подачу електроенергії. Всі спроби зупинити цей катастрофічний процес нічого не дали. Подачу електроенергії було припинено. До того ж, хакери ще й відключили резервні джерела електропостачання, до яких були підключені самі диспетчери.

Спеціалісти зі США, які допомагали нашим спеціалістам відновлювати пошкоджену систему, оцінили кібератаку як високопрофесійно підготовлену і блискуче проведену операцію. Підтверджені тому є достатньо і крім знеструмлення Прикарпаття. Кібербезпека, питання захисту інформації потребують комплексного і системного підходу до успішного вирішення завдань цього напрямку.

Питання захисту прав людини в умовах зростання впливу інформаційно-телекомунікаційних технологій практично на всі сфери її життя чим далі, тим більше загострюється. Потребує постій-

ної роботи над законодавчою базою в такому ж темпі, в якому ці технології розвиваються. Оскільки розвиток технологій вносить свої корективи і у формат життя людини, суспільства і держави. Наприклад, поступова реалізація на практиці Концепції Інтернету речей. У період 2008–2009 рр. відбувся перехід від «Інтернету людей» до «Інтернету речей», тобто кількість підключених до мережі речей-пристроїв значно перевищило кількість користувачів. Інтернет речей є системою, в якій інтегровано реальний і віртуальний світ речей. Ці речі взаємозв'язані (об'єднані) між собою дротовими і бездротовими каналами зв'язку. Це штучно створений світ, у якому людина управляє, користується, спілкується з необхідними речами-пристроями.

До цього треба ставитися уважно із розумінням вже як до доведеного факту. Це реальність, яку не можна ігнорувати. Концепцією Інтернету речей передбачається, що «речі» в недалекому майбутньому повинні стати активними учасниками бізнесу, допомагаючи людині, брати участь в інформаційних і соціальних процесах, бути посередником між людиною і навколишнім простором, реагувати на зміни у світі без втручання людини.

Із розвитком Інтернету речей будуть з'являтися і нові можливості. Все більше речей-пристроїв будуть підключатися до глобальної мережі, а це сприятиме і покращенню контролю за рівнем безпеки, аналітики, управління. А суть твердження про контроль над рівнем безпеки, як варіант, може полягати в тому, що речі-пристрої, об'єднані в кіберпросторі, будуть здійснювати контроль над спробами проникнення загроз у таку інтегровану систему і своєчасно вмикати механізми захисту.

Це явище вже зараз вимагає до себе відповідної уваги. У цьому напрямі дуже багато питань, які потенційно мають досить проблемну перспективу. Це навіть важко уявити, за якими правилами, нормами й алгоритмами будуть регулюватися відносини між людьми, реальними та віртуальними речами в кіберсистемах різних рівнів. А в міжнародному правовому полі? Це при тому, що на законодавчому рівні в галузі й на сьогодні ще багато неврегульованих питань, а реальність уже диктує нові завдання: і технологічні, і нормативно-правові. Хоча, треба відзначити, рух у цьому напрямі є. Наприклад, прийнято Закон України «Про доступ до публічної інформації». Цим зроблено важливий і необхідний крок. Із прийняттям Закону значно спрощено комунікацію між державою та її громадянами. Це дуже важливо щодо подальшої інформатизації суспільства.

Якість життя населення буде покращуватися. Але й безпека буде лишатися під знаком запитання, якщо на технологічному рівні не буде вирішено проблему захисту. Нікола Тесла ще у 1926 році в інтерв'ю журналу «Collier's» зробив прогноз на майбутнє, що радіо буде перетворено на «великий мозок», всі речі ста-

нуть частиною єдиного цілого, а інструменти, завдяки яким це стане можливим, будуть легко поміщатися в кишені. І перше, куди було спрямовано цей ресурс стала економіка.

У наш час технології розвиваються дуже швидко як у кількісному розумінні, так і в принципово якісному. Як наслідок, радикально змінюються формати життєдіяльності, особливо у напрямі використання ресурсів. А іноді відмова від ресурсів як таких, що стають більш затратними для обслуговування. У якості прикладу можна навести заміну на роботів працівників на одному з промислових підприємств Китаю в місті Дунгуань. Було 650 працівників, залишилося 60, які вже виробництвом продукції не займалися, це почали робити роботи, а обслуговували роботів. Підприємство почало працювати більш динамічно, більш продуктивно, більш якісно і значно з більшим прибутком.

Однак ідеалізувати таке майбутнє також не треба, ми тільки починаємо входити в інтегрований світ інтернету і достатнього досвіду в нас поки немає. Використання такого потужного ресурсу як Інтернет в інтересах економічного розвитку, великої мережі з її можливостями контролювати світ та глобальна відкритість даних несе в собі й загрози. І насамперед щодо економічної безпеки.

**Висновки.** До основних висновків можна віднести такі позиції:

– Україна знаходиться в процесі інтеграції в європейський ринок інформаційно-комунікаційних технологій – це факт. Інша справа, що темпи інтеграції низькі;

– спостерігаються позитивні зрушення щодо узгодження та врегулювання функцій держави і ринку ІКТ; органи влади поставлені перед необхідністю зробити розвиток телекомунікаційної галузі державним пріоритетом;

– інвестиційна непривабливість України зумовлена слабкістю системи кіберзахисту;

– рівень економічної безпеки телекомунікаційних підприємств залишається слабким через організаційну та політико-правову неврегульованість у середині держави.

Остання позиція у висновках, а саме політика-правова та організаційна неврегульованість між галуззю телекомунікацій та органами державної влади і, як наслідок, низький рівень економічної безпеки телекомунікаційних підприємств представляє, на думку автора, науковий інтерес на перспективу.

#### БІБЛІОГРАФІЧНИЙ СПИСОК:

1. Реформи галузі інформаційно-комунікаційних технологій та розвиток інформаційного простору України: матеріали парламентських слухань у Верховній Раді України 3 лютого 2016 р. / Верховна Рада України, Комітет з питань інформатизації та зв'язку; ред. кол.: О. Данченко (голова), Г. Андрощук, О. Старинець, О. Баранов [та ін.]. – К.: Парлам.вид-во, 2016. – 256 с.
2. Янковский А. Проблемы в сфере кибербезопасности в Украине. [Електронний ресурс] // Украинская правда. – Режим доступа: <http://www.pravda.com.ua/rus/columns/2017/02/15/7135442/>.
3. Зубко Т. Оцінка рівня економічної безпеки підприємства галузі зв'язку / Т. Зубко // Економіка. Менеджмент. Бізнес. – № 3(17). – 2016. – К.: ДУТ. – С. 81–87.
4. Новикова І. Управління конкурентоспроможністю телекомунікаційних підприємств: теорія, методологія, практика: монографія / І. Новикова. – Миколаїв: ФОП В. Швець, 2013. – 296 с.
5. Гудзь О. Гармонізація механізму стратегічного управління інноваційним розвитком підприємства [Електронний ресурс] // Глобальні та національні проблеми економіки. – 2015. – № 3. – Режим доступа: <http://global-national.in.ua/>. – С. 26–32.
6. Макаренко Т. Стратегія забезпечення інвестиційної безпеки малого та середнього бізнесу в Україні (на прикладі франчайзингу) / Т. Макаренко // Науково-аналітичний щоквартальний збірник Національного інституту стратегічних досліджень «Стратегічні пріоритети». – Київ, 2016. – Випуск № 1(38). – С. 78–85.
7. Ястремская Н., Фролова Л. Развитие информационного рынка как условие и результат становления информационной экономики. [Електронний ресурс] // Инженерный вестник Дона. – № 4 (27) / Том 27 / 2013. – Режим доступа: <http://cyberleninka.ru/article/n/razvitie-informatsionnogo-rynka-kak-uslovie-i-rezultat-stanovleniya-informatsionnoy-ekonomiki>.